

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES
PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro



(43) Internationales Veröffentlichungsdatum
5. Juli 2001 (05.07.2001)

PCT

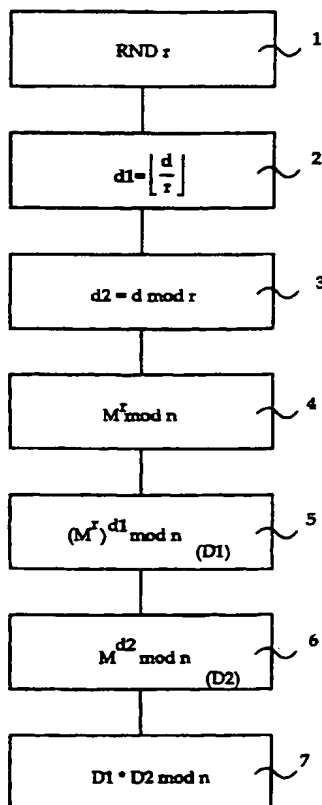
(10) Internationale Veröffentlichungsnummer
WO 01/48974 A1

- (51) Internationale Patentklassifikation⁷: H04L 9/30, G06F 7/72 (72) Erfinder; und
(75) Erfinder/Anmelder (nur für US): DREXLER, Hermann [DE/DE]; Oberländerstrasse 5a, 81371 München (DE).
(21) Internationales Aktenzeichen: PCT/EP00/13031 VATER, Harald [DE/DE]; An den Schulgärten 23, 35398 Giessen (DE).
(22) Internationales Anmeldedatum: 20. Dezember 2000 (20.12.2000) (74) Anwalt: KLUNKER, SCHMITT-NILSON, HIRSCH; Winzererstr. 106, 80797 München (DE).
(25) Einreichungssprache: Deutsch (81) Bestimmungsstaaten (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.
(26) Veröffentlichungssprache: Deutsch
(30) Angaben zur Priorität: 199 63 408.4 28. Dezember 1999 (28.12.1999) DE
(71) Anmelder (für alle Bestimmungsstaaten mit Ausnahme von US): GIESECKE & DEVRIENT GMBH [DE/DE]; Prinzregentenstrasse 159, 81677 München (DE).

[Fortsetzung auf der nächsten Seite]

(54) Title: PORTABLE DATA CARRIER PROVIDED WITH ACCESS PROTECTION BY DIVIDING UP CODES

(54) Bezeichnung: TRAGBARER DATENTRÄGER MIT ZUGRIFFSSCHUTZ DURCH SCHLÜSSELTEILUNG



(57) Abstract: The invention relates to a data carrier comprising a semiconductor chip provided with at least one memory in which an operating program is stored. Said operating program contains a number of instructions, whereby each instruction is elicited by signals that can be detected outside of the semiconductor chip. The aim of the invention is to protect secret data, which is provided in the chip of the data carrier, from "Differential Power Analysis" (DPA) or Higher Order DPA. To this end, the invention provides that in order to carry out security-relevant operations in the semiconductor chip, the data carrier is designed for dividing up secret data, which is stored or generated by the same, into at least three data parts, whereby an arithmetic unit for calculating a random number and for dividing the random number is contained therein, whereby the first data part is the integer result of the division, the second part is the remainder of the division, and the third part is the random number itself.

(57) Zusammenfassung: Die Erfindung betrifft einen Datenträger mit einem Halbleiterchip der wenigstens einen Speicher aufweist, in dem ein Betriebsprogramm abgelegt ist, das mehrere Befehle beinhaltet, wobei jeder Befehl von ausserhalb des Halbleiterchips detektierbare Signale hervorruft. Es ist Aufgabe der Erfindung, geheime Daten, die im Chip des Datenträgers vorhanden sind, vor "Differential Power Analysis" (DPA) bzw. Higher Order DPA zu schützen. Gemäss der Erfindung ist der Datenträger ausgelegt, um zur Durchführung sicherheitsrelevanter Operationen im Halbleiterchip abgelegte oder von diesem generierte geheime Daten in mindestens drei Datenteile aufzuteilen, wobei eine Recheneinheit zum Berechnen einer Zufallszahl und zur Teilung der Zufallszahl enthalten ist, wobei der erste Datenteil das ganzzahlige Ergebnis der Teilung ist, der zweite Teil der Rest der Teilung und der dritte Teil die Zufallszahl selbst ist.

WO 01/48974 A1



(84) **Bestimmungsstaaten (regional):** ARIPO-Patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI-Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

— Mit internationalem Recherchenbericht.

Zur Erklärung der Zweibuchstaben-Codes, und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

Tragbarer Datenträger mit Zugriffsschutz durch Schlüsselteilung

- 5 Die Erfindung betrifft einen Datenträger, der einen Halbleiterchip aufweist, in dem geheime Daten abgespeichert sind und verarbeitet werden.

Datenträger die einen Chip enthalten, werden in einer Vielzahl von unterschiedlichen Anwendungen eingesetzt, beispielsweise zum Durchführen von

10 Finanztransaktionen, zum Bezahlen von Waren oder Dienstleistungen, oder als Identifikationsmittel zur Steuerung von Zugangs- oder Zutrittskontrollen. Bei allen diesen Anwendungen werden innerhalb des Chips des Datenträgers in der Regel geheime Daten verarbeitet, die vor dem Zugriff durch unberechtigte Dritte geschützt werden müssen. Dieser Schutz wird unter

15 anderem dadurch gewährleistet, daß die inneren Strukturen des Chips sehr kleine Abmessungen aufweisen und daher ein Zugriff auf diese Strukturen mit dem Ziel, Daten, die in diesen Strukturen verarbeitet werden, auszuspähen, sehr schwierig ist. Um einen Zugriff weiter zu erschweren, kann der Chip in eine sehr fest haftende Masse eingebettet werden, bei deren gewaltsamer Entfernung das Halbleiterplättchen zerstört wird oder zumindest die

20 darin gespeicherten geheimen Daten vernichtet werden. Ebenso ist es auch möglich, das Halbleiterplättchen bereits bei dessen Herstellung mit einer Schutzschicht zu versehen, die nicht ohne Zerstörung des Halbleiterplättchens entfernt werden kann.

25

Mit einer entsprechenden technischen Ausrüstung, die zwar extrem teuer aber dennoch prinzipiell verfügbar ist, könnte es einem Angreifer möglicherweise gelingen, die innere Struktur des Chips freizulegen und zu untersuchen. Das Freilegen könnte beispielsweise durch spezielle Ätzverfahren

30 oder durch einen geeigneten Abschleifprozeß erfolgen. Die so freigelegten Strukturen des Chips, wie beispielsweise Leiterbahnen, könnten mit Mikro-

sonden kontaktiert oder mit anderen Verfahren untersucht werden, um die Signalverläufe in diesen Strukturen zu ermitteln. Anschließend könnte versucht werden, aus den detektierten Signalen geheime Daten des Datenträgers, wie z.B. geheime Schlüssel zu ermitteln, um diese für Manipulationszwecke einzusetzen. Ebenso könnte versucht werden, über die Mikrosonden die Signalverläufe in den freigelegten Strukturen gezielt zu beeinflussen.

In jüngerer Zeit sind überdies Methoden bekannt geworden, die es erlauben durch die Messung der Stromaufnahme oder des Zeitverhaltens bei der Verschlüsselung auf die geheimen Daten, insbesondere den geheimen Schlüssel zu schließen (Paul C. Kocher, „Timing attacks on implementation of Diffie-Hellman, RSA, DSS, and other Systems“, Springer Verlag 1998; WO 99/35782).

Ein einfacher derartiger Angriff besteht in der „Simple Power Analysis“ (SPA). Bei dieser Analysemethode wird beispielsweise eine bekannte Nachricht M einer Verschlüsselung mit einem geheimen Schlüssel d unterzogen, d.h. es wird der verschlüsselte Text $Y = M^d \bmod n$ gebildet. Bei der modularen Exponentiation wird bei einer „1“ im Exponenten d eine Quadrier-Operation mit dem Zwischenergebnis und eine Multilizier-Operation mit M durchgeführt, während bei einer „0“ in d nur eine Quadrier-Operation mit dem Zwischenergebnis ausgeführt wird. Bei bekanntem M kann durch die Beobachtung des Strom und/oder Zeitverhaltens während der Operationen die Nachricht M erkannt werden. Da diese immer bei Vorliegen einer „1“ in d verwendet wird, kann ohne weiteres auf den Schlüssel geschlossen werden.

Diesem Angriff kann ohne weiteres durch einfache Änderungen in der Nachricht M bzw. im Schlüssel d begegnet werden. Aus Paul C. Kocher, „Timing Attacks on implementation of Diffie-Hellman, RSA, DSS, and other

Systems", Springer Verlag 1998 und der internationalen Patentanmeldung WO 99/35782 sind weitere Analysemethoden bekannt, bei denen auch bei geänderter, d.h. verschleierter Nachricht oder verschleiertem Schlüssel durch die Aufnahme einer Vielzahl von Meßkurven, in denen das Stromverhalten des integrierten Schaltkreises gemessen wird auf den Schlüssel geschlossen werden kann („Differential Power Analysis" (DPA) bzw. Higher Order DPA).

Als Sicherungsmaßnahme wurde ein sogenanntes „Exponent Blinding" vorgeschlagen, bei dem der geheime Schlüssel d nicht direkt verwendet wurde.

Zum einen kann anstelle des geheimen Schlüssels d für die Verschlüsselung $d+r*\Phi$ verwendet werden, wobei r eine Zufallszahl und Φ die Eulersche PHI-Funktion ist. Speziell für den RSA-Algorithmus gilt: $n = p*q$, wobei p und q Primzahlen sind und somit $\Phi = (p-1)*(q-1)$ ist. Unter Anwendung des Eulers-Theorem gilt: $M^d \bmod n = M^{d+r*\Phi} \bmod n$.

Wenn bei jeder Berechnung eine andere Zufallszahl r verwendet wird, kann auch bei einer Vielzahl von Analyse-Reihen nicht auf den Schlüssel d geschlossen werden.

Alternativ kann der geheime Schlüssel d in $d_1*d_2 \bmod \Phi$ zerlegt werden. Es wird für die Verschlüsselung $Y = M^{d_1*d_2 \bmod \Phi} \bmod n = (M^{d_1})^{d_2} \bmod n$.

Der Nachteil dieser Schutzmöglichkeit besteht jedoch darin, daß aus Mangel an Speicherplatz die Primzahlen p und q oder Φ üblicherweise nicht in einer Chipkarte abgelegt sind.

Der geheime Schlüssel d kann auch in eine Summe aus d_1 und d_2 zerlegt werden. Es gilt dann $d = d_1 + d_2$ bzw. für die Verschlüsselung:

$$Y = M^{d_1+d_2} \bmod n = M^{d_1} * M^{d_2} \bmod n = (M^{d_1} \bmod n * M^{d_2} \bmod n) \bmod n.$$

- Um eine ausreichend hohe Sicherheit zu erhalten, muß bei der Zerlegung des Exponenten in $d = d_1 + d_2$ oder $d = d_1 \cdot d_2 \bmod \Phi$ für jede Berechnung ein neues, zufälliges d_1/d_2 -Paar gewählt werden. Da die Erzeugung von Zufallszahlen in der Regel sehr langsam ist, eignet sich dieses Verfahren nicht zum Einsatz in Chipkarten. Zudem wird der Rechenaufwand für die modulare Exponentiation wesentlich erhöht, so daß auch dies gegen einen Einsatz in der Chipkarte spricht.
- 5
- 10 Es ist daher Aufgabe der Erfindung, geheime Daten, die im Chip eines tragbaren Datenträgers vorhanden sind, vor unberechtigtem Zugriff zu schützen, wobei der effiziente Einsatz der Daten nach wie vor gewährleistet sein soll.
- 15 Diese Aufgabe wird ausgehend vom Oberbegriff der Ansprüche 1 bzw. 7 und 12 durch die kennzeichnenden Merkmale des jeweiligen Anspruchs gelöst.
- 20 Die Erfindung gibt einen Datenträger mit einem Halbleiterchip der wenigstens einen Speicher aufweist, in dem ein Betriebsprogramm abgelegt ist, das mehrere Befehle beinhaltet, wobei jeder Befehl von außerhalb des Halbleiterchips detektierbare Signale hervorruft, an.
- 25 Gemäß der Erfindung ist der Datenträger ausgelegt, um zur Durchführung sicherheitsrelevanter Operationen im Halbleiterchip abgelegte oder von diesem generierte geheime Daten in mindestens drei Datenteile aufzuteilen. Er enthält eine Rechner- bzw. Recheneinheit zum Berechnen einer Zufallszahl und zur Teilung der geheimen Daten durch die Zufallszahl. Der erste Datenteil besteht aus dem ganzzahligen Ergebnis der Teilung, der zweite Teil ist

durch den Rest der Teilung gegeben und der dritte Datenteil ist die Zufallszahl selbst.

5 Gemäß einer vorteilhaften Ausgestaltung der Erfindung bestehen die geheimen Daten aus dem geheimen Schlüssel für eine Verschlüsselung von Nachrichten, wobei vorzugsweise der geheime Schlüssel als Exponent bei der Berechnung von Gruppen-Operationen in asymmetrischen Verschlüsselungsverfahren (public-key-Verfahren, z.B. elliptische Kurven, RSA, usw.) bzw. von Modulo-Operationen eingesetzt wird.

10 Eine weitere Ausgestaltung der Erfindung sieht vor, daß die Zufallszahl so gewählt wird, daß die Länge der Zufallszahl zusammen mit dem Hamminggewicht der Zufallszahl bei verschiedenen Zufallszahlen etwa konstant ist. Auf diese Weise wird erreicht, daß aus der Zeitdauer, welche für die modulare Exponentiation, die proportional zur Länge des Exponenten und dem
15 Hamminggewicht des Exponenten ist, nicht auf die geheimen Daten geschlossen werden kann.

20 Das erfindungsgemäße Verfahren sieht vor, daß der geheime Schlüssel durch eine vergleichsweise kurze Zufallszahl geteilt wird. Das Teilungsergebnis ohne Rest ergibt den ersten Teil des Schlüssels, der Rest ergibt den zweiten Teil des Schlüssels und die Zufallszahl den dritten Teil.

25 Für die Verschlüsselung einer Nachricht M gilt $Y = M^d \bmod n$. Der geheime Schlüssel d wird in d_1 , d_2 und r aufgeteilt, wobei $d_1 = d/r$ (r ist eine Zufallszahl) ohne Rest gilt. Der Rest der Teilung ist der zweite Teil d_2 des Schlüssels d . Damit gilt $d_2 = d \bmod r$. Für den Schlüssel d gilt somit $d = r \cdot d_1 + d_2$.

Damit ergibt sich ein Verschlüsselungstext

- 6 -

$$Y = M^d \bmod n = M^{r^{d_1} + d_2} \bmod n = (M^r)^{d_1} * M^{d_2} \bmod n = \\ = ((M^r)^{d_1} \bmod n * M^{d_2} \bmod n) \bmod n.$$

Der Ablauf der Bildung des verschlüsselten Textes Y ist in Fig. 1 dargestellt.

5

In Schritt 1 wird zunächst eine Zufallszahl r gebildet. Anschließend wird in Schritt 2 aus dem geheimen Schlüssel d durch Teilung mit der zuvor erhaltenen Zufallszahl r der erste Schlüsselteil d₁ berechnet. Der zweite Teil d₂ des Schlüssels wird durch Bildung von d mod r erhalten.

10

In Schritt 4 wird mit der Berechnung des Verschlüsselungstextes begonnen, indem zunächst $M^r \bmod n$ berechnet wird. Im nächsten Schritt 5 wird $D_1 = (M^r)^{d_1} \bmod n$ und in Schritt 6 wird $D_2 = M^{d_2} \bmod n$ berechnet.

15 Die Reihenfolge der einzelnen Rechenoperationen kann natürlich zum Teil auch zeitlich vertauscht werden. So kann zuerst $M^{d_1} \bmod n$ berechnet werden und dann $(M^{d_1})^r \bmod n$, da $(M^r)^{d_1} \bmod n = (M^{d_1})^r \bmod n$ ist.

Im letzten Schritt 7 werden die Zwischenergebnisse D₁ und D₂ miteinander
20 multipliziert und der Modulo zu n gebildet. Es gilt damit

$$D_1 * D_2 \bmod n = M^d \bmod n = Y.$$

Die Erfindung hat den Vorteil, daß weder die Primzahlen p und q zur Bildung von Φ in der Karte gespeichert sein müssen und auch die Erzeugung
25 langer Zufallszahlen, die sehr viel Rechenzeit in Anspruch nimmt, vermieden wird. Es wird weiterhin der Rechenaufwand für die Modulo-Operationen in Grenzen gehalten, so daß die erfindungsgemäße Lösung sowohl sicher als auch effizient in einer Chipkarte eingesetzt werden kann.

30 Weiterhin müssen bei dem beschriebenen Verfahren keine Daten im nicht-

- 7 -

flüchtigen Speicher des Datenträgers abgeändert werden, was Zeit beanspruchen und zu einem Degradieren des nichtflüchtigen Speichers führen würde.

- 5 Da eine modulare Exponentiation eine Zeitdauer benötigt, die proportional zur Länge des Exponenten und des Hamminggewichts des Exponenten ist, kann eine zusätzliche Erhöhung der Sicherheit erreicht werden, wenn für die Erzeugung der Zufallszahl r ein Verfahren gewählt wird, bei der die Länge von r und das Hamminggewicht von r eine Konstante ergibt.

10

Die Erfindung kann für eine Vielzahl von Verschlüsselungssysteme angewendet werden. Es sei beispielhaft auf die RSA-Verschlüsselung, die Verschlüsselung nach ElGamal, DSA, Elliptische Kurvensysteme usw. verwiesen.

15

Patentansprüche

1. Datenträger mit einem Halbleiterchip der wenigstens einen Speicher aufweist, in dem ein Betriebsprogramm abgelegt ist, das mehrere Befehle
5 beinhaltet, wobei jeder Befehl von außerhalb des Halbleiterchips detektierbare Signale hervorruft, dadurch gekennzeichnet, daß der Datenträger ausgelegt ist, um zur Durchführung sicherheitsrelevanter Operationen im Halbleiterchip abgelegte oder von diesem generierte geheime Daten in mindestens drei Datenteile aufzuteilen, wobei eine Recheneinheit zum Berechnen einer Zufallszahl und zur Teilung der Zufallszahl enthalten ist, wobei
10 der erste Datenteil das ganzzahlige Ergebnis der Teilung ist, der zweite Teil der Rest der Teilung und der dritte Teil die Zufallszahl selbst ist.
2. Datenträger nach Anspruch 1, dadurch gekennzeichnet, daß die geheimen Daten ein geheimer Schlüssel für eine Verschlüsselung von Nachrichten
15 sind.
3. Datenträger nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß die geheimen Daten als Exponent bei der Berechnung von Gruppen-
20 Operationen in asymmetrischen Verschlüsselungsverfahren Verwendung finden.
4. Datenträger nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß die geheimen Daten als Exponent bei der Berechnung von Modulo-
25 Operationen eingesetzt werden.
5. Datenträger nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß der geheime Schlüssel als Exponent bei der Berechnung von Modulo-Operationen eingesetzt wird.

6. Datenträger nach einem der Ansprüche 1 - 5, dadurch **gekennzeichnet**, daß die Zufallszahl so gewählt wird, daß die Länge der Zufallszahl zusammen mit dem Hamminggewicht der Zufallszahl bei verschiedenen Zufallszahlen etwa konstant ist.

5

7. Verfahren zur Sicherung geheimer Daten in Datenträgern mit einem Halbleiterchip der wenigstens einen Speicher aufweist, in dem ein Betriebsprogramm abgelegt ist, das mehrere Befehle beinhaltet, wobei jeder Befehl von außerhalb des Halbleiterchips detektierbare Signale hervorruft, dadurch **gekennzeichnet**, daß zur Durchführung sicherheitsrelevanter Operationen im Halbleiterchip abgelegte oder von diesem generierte geheime Daten in mindestens drei Datenteile aufgeteilt werden, wobei zunächst eine Zufallszahl berechnet wird und der erste Datenteil aus dem ganzzahligen Ergebnis einer Teilung der geheimen Daten durch die Zufallszahl ist, der
10 zweite Teil aus dem Rest der Teilung besteht und der dritte Teil die Zufallszahl selbst ist.

15

8. Verfahren nach Anspruch 7, dadurch **gekennzeichnet**, daß die geheimen Daten ein geheimer Schlüssel für eine Verschlüsselung von Nachrichten
20 sind.

20

9. Verfahren nach Anspruch 7 oder 8, dadurch **gekennzeichnet**, daß die geheimen Daten als Exponent bei der Berechnung von Gruppen-Operationen in asymmetrischen Verschlüsselungsverfahren Verwendung finden.

25

10. Verfahren nach Anspruch 7 oder 8, dadurch **gekennzeichnet**, daß die geheimen Daten als Exponent bei der Berechnung von Modulo-Operationen eingesetzt werden.

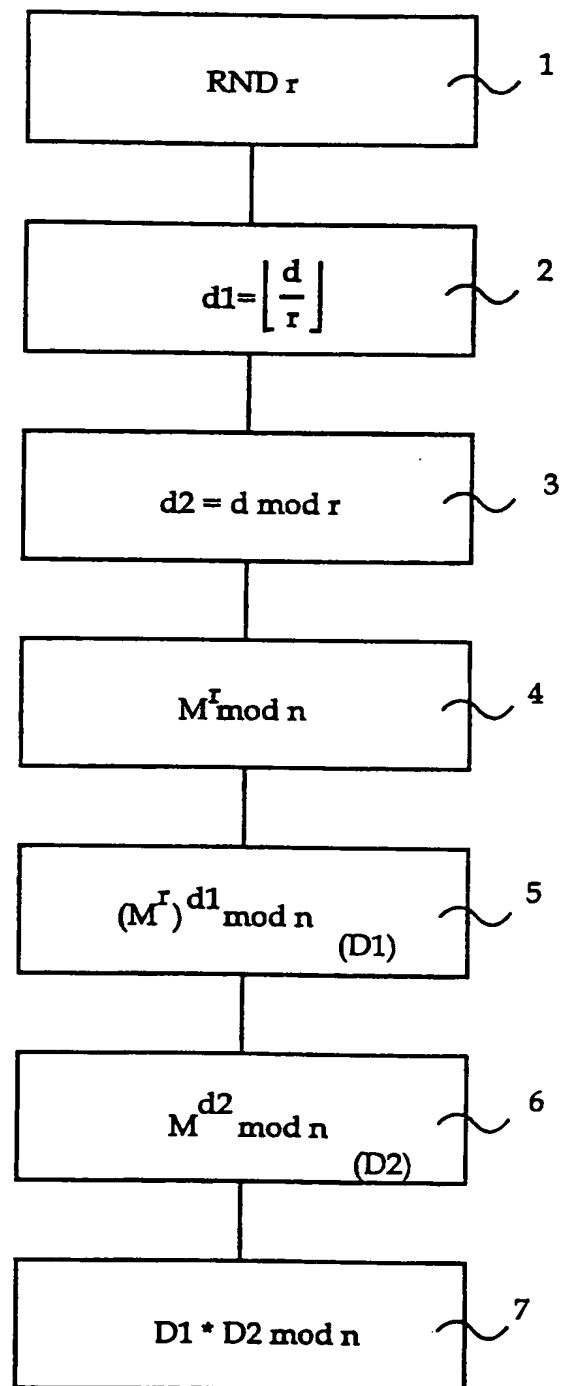
11. Verfahren nach Anspruch 7 oder 8, dadurch **gekennzeichnet**, daß der geheime Schlüssel als Exponent bei der Berechnung von Modulo-Operationen eingesetzt wird.
- 5 12. Verfahren nach einem der Ansprüche 7 - 11, dadurch **gekennzeichnet**, daß die Zufallszahl so gewählt wird, daß die Länge der Zufallszahl zusammen mit dem Hamminggewicht der Zufallszahl bei verschiedenen Zufallszahlen etwa konstant ist.
- 10 13. Verfahren zur Bildung einer verschlüsselten Nachricht in einem System zur Authentisierung von Systemkomponenten oder zur Bildung einer Signatur, dadurch **gekennzeichnet**, daß
- eine Zufallszahl r gebildet wird,
 - aus einem geheimen Schlüssel d durch Teilung mit der zuvor erhaltenen

15 Zufallszahl r ein erster Schlüsselteil (d_1) berechnet wird,

 - ein zweiter Teil (d_2) des Schlüssels durch Bildung von $d \bmod r$ erhalten wird,
 - mit der Berechnung des Verschlüsselungstextes begonnen wird, indem $M^r \bmod n$ berechnet wird,

20 - $D1 = (M^r)^{d_1} \bmod n$ und $D2 = M^{d_2} \bmod n$ berechnet wird und

 - die Zwischenergebnisse $D1$ und $D2$ miteinander multipliziert und der Modulo zu n gebildet wird.
14. Verfahren nach Anspruch 13, dadurch **gekennzeichnet**, daß zur Berechnung von $D1$ zunächst $M^{d_1} \bmod n$ und nachfolgend $(M^{d_1})^r \bmod n$ berechnet wird.
- 25



INTERNATIONAL SEARCH REPORT

International Application No

PCT/EP 00/13031

A. CLASSIFICATION OF SUBJECT MATTER

IPC 7 H04L9/30 G06F7/72

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, INSPEC, PAJ, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	<p>KOCHER P C: "TIMING ATTACKS ON IMPLEMENTATIONS OF DIFFIE-HELLMAN, RSA, DSS, AND OTHER SYSTEMS" 16TH. ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE. SANTA BARBARA, AUG. 18 - 22, 1996. PROCEEDINGS, BERLIN, SPRINGER, DE, vol. CONF. 16, 18 August 1996 (1996-08-18), pages 104-113, XP000626590 ISBN: 3-540-61512-1 cited in the application page 111 -page 112</p> <p style="text-align: center;">---</p> <p style="text-align: center;">-/--</p>	1-14



Further documents are listed in the continuation of box C.



Patent family members are listed in annex.

* Special categories of cited documents :

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

- *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- *&* document member of the same patent family

Date of the actual completion of the international search

28 March 2001

Date of mailing of the international search report

06/04/2001

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax (+31-70) 340-3016

Authorized officer

Carnerero Álvaro, F

INTERNATIONAL SEARCH REPORT

Internat. Application No

PCT/EP 00/13031

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	<p>MESSERGES T S ET AL: "Power analysis attacks of modular exponentiation in smartcards"</p> <p>CRYPTOGRAPHIC HARDWARE AND EMBEDDED SYSTEMS. INTERNATIONAL WORKSHOP, XX, XX, August 1999 (1999-08), pages 144-157, XP000952221</p> <p>page 155 -page 156</p>	1-14

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen

PCT/EP 00/13031

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 H04L9/30 G06F7/72

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RESEARCHIERTE GEBIETE

Researchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)

IPK 7 H04L G06F

Researchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die researchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

EPO-Internal, INSPEC, PAJ, WPI Data

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	<p>KOCHER P C: "TIMING ATTACKS ON IMPLEMENTATIONS OF DIFFIE-HELLMAN, RSA, DSS, AND OTHER SYSTEMS"</p> <p>16TH. ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE. SANTA BARBARA, AUG. 18 - 22, 1996. PROCEEDINGS, BERLIN, SPRINGER, DE, Bd. CONF. 16,</p> <p>18. August 1996 (1996-08-18), Seiten 104-113, XP000626590</p> <p>ISBN: 3-540-61512-1</p> <p>in der Anmeldung erwähnt</p> <p>Seite 111 -Seite 112</p> <p style="text-align: center;">---</p> <p style="text-align: center;">-/-</p>	1-14

☒ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☐ Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung, die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung, die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"Z" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

28. März 2001

Absenddatum des internationalen Recherchenberichts

06/04/2001

Name und Postanschrift der internationalen Recherchenbehörde

Europäisches Patentamt, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax (+31-70) 340-3016

Bevollmächtigter Beauftragter

Carnerero Álvaro, F

INTERNATIONALER RECHERCHENBERICHT

Interns .ales Aktenzeichen

PCT/EP 00/13031

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	<p>MESSERGES T S ET AL: "Power analysis attacks of modular exponentiation in smartcards"</p> <p>CRYPTOGRAPHIC HARDWARE AND EMBEDDED SYSTEMS. INTERNATIONAL WORKSHOP, XX, XX, August 1999 (1999-08), Seiten 144-157, XP000952221</p> <p>Seite 155 -Seite 156</p> <p>-----</p>	1-14



Europäisches
Patentamt
European Patent
Office
Office européen des
brevets

Description of WO0148974

Print

Copy

Contact Us

Close

Result Page

Notice: This translation is produced by an automated process; it is intended only to make the technical content of the original document sufficiently clear in the target language. This service is not a replacement for professional translation services. The esp@cenet® Terms and Conditions of use are also applicable to the use of the translation tool and the results derived therefrom.

Portable data carrier with < RTI ID=1.1> Zugriffsschutz< /RTI> by allotting pro rata hurrying the invention relates to a data carrier, which exhibits a semiconductor chip, become processed in which secret data stored are and.

Data carriers the one chip contained, become inserted, for example accomplishing by financial transactions, in a variety of different applications, paying merchandise or services, or as identification means the control of Zugangs- oder admission controls. With all these applications become processed within the chip of the data carrier usually secret data, which before the access by unauthorized third protected to become to have. This protection becomes among other things ensured by the fact that the internal structures of the chip exhibit much small dimensions and therefore an access to these structures with the target, data, which become processed in these structures < RTI ID=1.2> auszuspä < /RTI> hen, very difficult is. In order to make access more difficult more other, the chip can become into a very fixed adhesive bulk embedded, with of them removal by force < RTI ID=1.3> Halbleiterplättchen< /RTI> destroyed will be destroyed or at least the secret data stored therein. Likewise it is < also possible, that; RTI ID=1.4> Halbleiterplättchen< /RTI> already with its manufacturing with a protective layer to provide, those not without destruction < RTI ID=1.5> Halbleiterplätt < /RTI> chens remote will can.

With a corresponding technical equipment, which is more available nevertheless in principle extreme expensively however, it could an aggressor < RTI ID=1.6> mögli < /RTI> cherweise succeed to open and examine the internal structure of the chip. Opening could for example by particular etching processes or by an appropriate < RTI ID=1.7> Abschleifprozess< /RTI> take place. In such a way opened structures of the chip, as for example conductive traces, could become with micro probes contacted or with other methods examined, in order to determine the signal processes in these structures. Subsequent one could become attempted, from that detected signals secret data < RTI ID=2.1> Datenträ < /RTI> gers, like z. B. to determine secret key, in order to use these for manipulation purposes. Likewise attempted could become to affect over the Mikrosonden the signal processes in the opened structures targeted.

In younger time besides methods became known, it permit by the measurement of the power input or the time performance with the Ver< RTI ID=2.2> schlüsselung< /RTI> on the secret data to close in particular the secret key (Paul C. Cooke, "timing attacks on implementation OF Diffie Hellman, RSA, dss, and OTHER of system", Springer Verlag 1998; WHERE 99/35782).

A simple such attack exists in the " simple power analysis " (SPA). With this analysis method for example a known message M of an encryption with a secret key D is submitted, of D. h. it becomes the encrypted text $Y = MD \bmod n$ formed. With the modular Exponentiation with one < RTI ID=2.3> a " 1 " im< /RTI> Exponent D one square operation with the intermediate result and an Multilizer operation with M performed, while with < RTI ID=2.4> " 0 " in< /RTI> D only a squaring operation with < RTI ID=2.5> Zwischenergebnis< /RTI> executed becomes. With known M stream can become and/or time performance during the operations the message M recognized by the observation. Since this always becomes when being present a " 1 " in D used, easily closed can become on the key.

▲ top

This attack can easily by simple changes in the message M and/or. in the key D to be met.



Europäisches
Patentamt
European Patent
Office
Office européen des
brevets

Claims of WO0148974

[Print](#)

[Copy](#)

[Contact Us](#)

[Close](#)

Result Page

Notice: This translation is produced by an automated process; it is intended only to make the technical content of the original document sufficiently clear in the target language. This service is not a replacement for professional translation services. The esp@cenet® Terms and Conditions of use are also applicable to the use of the translation tool and the results derived therefrom.

Claims 1. Data carrier with a semiconductor chip that at least a memory exhibits, is deposited in which an operating programme, several instructions the included, whereby each instruction of outside of the semiconductor chip causes detectable signals, characterised in that of the data carriers designed is, in order to divide to the feedthrough of safety-relevant operations in the semiconductor chip put down or from this generated secret data into at least three data parts, whereby an arithmetic unit is contained of a random number for calculation and for the division of the random number, whereby the first data part is the integral result of the division, which is second part the remainder of the division and the third part the random number.

2. Data carriers according to claim 1, characterised in that the secret data a secret key for an encryption from messages are.

3. Data carriers according to claim 1 or 2, characterised in that the secret data as exponent with the calculation of groups operations in asymmetrischen Verschlüsselungsverfahren use find.

4. Data carriers after one of the claims 1 to 3, characterised in that the secret data as exponent with the calculation of modulo operations inserted become.

5. Data carrier after one of the claims 1 to 3, characterised in that the secret keys as exponent with the calculation of modulo operations inserted becomes.

6. Data carrier after one of the claims 1-5, characterised in that the random number so chosen becomes that the length of the random number as well as the Hamminggewicht of the random number is constant with various random numbers.

7. Method to the fuse of secret data in < RTI ID=9.1> Datenträgern < /RTI> with a semiconductor chip that at least a memory exhibits, in a Be< RTI ID=9.2> triebsprogramm< /RTI> deposited is, several instructions included, whereby each instruction causes detectable signals of outside of the semiconductor chip, characterised in that to the feedthrough safety-relevant operations in the semiconductor chip put down or from this generated secret data into at least three data parts divided becomes, whereby first a random number becomes calculated and the first data part from the integral result of a division of the secret data is by the random number, which second part from the remainder of the division exists and which is third part the random number.

8. Process according to claim 7, characterised in that the secret data a secret key for an encryption from messages is.

9. Process according to claim 7 or 8, characterised in that the secret data as exponent with the calculation of group operations in asymmetrischen coding procedures use finds.

10. Process according to claim 7 or 8, characterised in that the secret data as exponent with the calculation of modulo operations inserted becomes.

▲ top

11. Process according to claim 7 or 8, characterised in that the secret keys as exponent with the calculation of modulo operations inserted becomes.

12. Process according to one of claims 7-11, characterised in that the random number so chosen becomes that the length of the random number as well as < RTI ID=10.1> Hamminggewicht < /RTI> the random number with various random numbers constant is.

13. Method to the formation of an encrypted message in a system to the authentication of system components or to the formation of a signature, characterised in that - a random number r formed becomes, - from a secret key D by division with the before obtained

Random number r first < RTI ID=10.2> Schlüsselteil < /RTI> < RTI ID=10.3> $(d1)$ < /RTI> calculated is < , - a second part $(d2)$ of the key by formation of $D \bmod r$ obtained becomes, - with the calculation; RTI ID=10.4> Verschlüsselungstextes < /RTI> started becomes, as M_r becomes mod n calculated, - $D1 = < RTI ID=10.5> (M_r) < /RTI> \bmod n$ and $D2 = M_{d2} \bmod n$ calculated becomes and - the intermediate results $D1$ and $D2$ multiplied with one another and that Modulo to n formed becomes.

14. Process according to claim 13, characterised in that for the calculation of $D1$ first $M_{d1} \bmod n$ and subsequent < RTI ID=10.6> $(M_{d1}) < /RTI> r \bmod n$ counts becomes.